Technical Specifications Manual for Online Testing

For Technology Coordinators

2014–2015

Published February 23, 2015

Prepared by the American Institutes for Research®

|  |  |
| --- | --- |
|  | [http://www.ode.state.oh.us/gd/templates/images/ODE/ohio_logo.gif](http://ohio.gov/) |

Table of Contents

[Introduction to the Technical Specifications Manual 1](#_Toc412474400)

[Manual Content 1](#_Toc412474401)

[Other Resources 1](#_Toc412474402)

[Section I. Network and Internet Requirements 3](#_Toc412474403)

[General Requirements 3](#_Toc412474404)

[Common Network Performance Bottlenecks 3](#_Toc412474405)

[Bandwidth 4](#_Toc412474406)

[Determining Bandwidth Requirements 5](#_Toc412474407)

[Total Number of Students Simultaneously Testing 5](#_Toc412474408)

[Size of the Test Content 5](#_Toc412474409)

[Secure Browser Installation 6](#_Toc412474410)

[Network Configuration 6](#_Toc412474411)

[Protocols 6](#_Toc412474412)

[Domain Name Resolution 6](#_Toc412474413)

[Content Filter, Firewalls, and Proxy Servers 6](#_Toc412474414)

[Quality of Service (QoS)/Traffic Shaping 7](#_Toc412474415)

[Certificate Revocation List 7](#_Toc412474416)

[Symantec Recommendations 7](#_Toc412474417)

[Wireless Networking 8](#_Toc412474418)

[Wireless Access Points 8](#_Toc412474419)

[Recommendations on the optimal number of student workstations per wireless connection 8](#_Toc412474420)

[Network Diagnostic Tools 9](#_Toc412474421)

[AIR’s Network/Bandwidth Diagnostic Tool 9](#_Toc412474422)

[Microsoft Windows Specific Tools 9](#_Toc412474423)

[Mac OS X Specific Tools 10](#_Toc412474424)

[Multi‐Platform Tools 10](#_Toc412474425)

[Section II. General Software Requirements 11](#_Toc412474426)

[Requirements for All Systems 11](#_Toc412474427)

[Enabling Pop-Up Windows 11](#_Toc412474428)

[Flash Information 12](#_Toc412474429)

[Windows Requirements 13](#_Toc412474430)

[Disabling Fast User Switching 13](#_Toc412474431)

[Disabling Fast User Switching in Windows XP 13](#_Toc412474432)

[Disabling Fast User Switching in Windows 7 13](#_Toc412474433)

[Disabling Fast User Switching in Windows 8.0 and 8.1 15](#_Toc412474434)

[Enabling Web Fonts in Internet Explorer 10 and 11 17](#_Toc412474435)

[Installing Windows Media Pack for Windows 8.1 N and KN 18](#_Toc412474436)

[Mac OS X Requirements 18](#_Toc412474437)

[Disabling Spaces 19](#_Toc412474438)

[Function Keys and Application Launches 20](#_Toc412474439)

[Disabling Spaces and Application Launches from the Command Line 21](#_Toc412474440)

[Disabling Spaces and Application Launches on Remote Machines 21](#_Toc412474441)

[Linux Requirements 22](#_Toc412474442)

[Installing Festival and Sound eXchange (SoX) Software 22](#_Toc412474443)

[Mobile Requirements 22](#_Toc412474444)

[iOS Requirements 23](#_Toc412474445)

[Guided Access 23](#_Toc412474446)

[Enabling Guided Access 23](#_Toc412474447)

[Configuring Using Autonomous Single App Mode 24](#_Toc412474448)

[Overview of Autonomous Single App Mode and the Secure Testing Environment 24](#_Toc412474449)

[Step 1: Creating a Mobile Device Management Profile 25](#_Toc412474450)

[Step 1a (Optional): Restricting Features in iOS 8.1.3 26](#_Toc412474451)

[Step 2: Creating a Supervisory Profile 27](#_Toc412474452)

[Step 3: Placing iPads in Autonomous Single App Mode 29](#_Toc412474453)

[Android Requirements 32](#_Toc412474454)

[Enabling the Secure Browser Keyboard 32](#_Toc412474455)

[Chrome OS Requirements 34](#_Toc412474456)

[Google Documentation 34](#_Toc412474457)

[Section III. Text-to-Speech Requirements 36](#_Toc412474458)

[Overview of Text-to-Speech 36](#_Toc412474459)

[Using Text-to-Speech 36](#_Toc412474460)

[How the Secure Browsers Work With Voice Packs 36](#_Toc412474461)

[Desktop Secure Browsers 36](#_Toc412474462)

[Mobile Secure Browsers 37](#_Toc412474463)

[About NeoSpeech™ Voice Packs for Windows 37](#_Toc412474464)

[Windows Text-to-Speech Settings 38](#_Toc412474465)

[Mac OS X Text-to-Speech Settings 39](#_Toc412474466)

[Linux Text-to-Speech Settings 40](#_Toc412474467)

[Voice Packs Recognized by Desktop Secure Browsers 41](#_Toc412474468)

[Windows 41](#_Toc412474469)

[Mac OS X 42](#_Toc412474470)

[Linux 43](#_Toc412474471)

[Appendix A. Systems and URLs Provided by AIR 44](#_Toc412474472)

[Non-Testing Sites 44](#_Toc412474473)

[Testing Sites 44](#_Toc412474474)

[TA and Student Testing Sites 44](#_Toc412474475)

[Appendix B. Technology Coordinator Checklist 45](#_Toc412474476)

[Appendix C. User Support 46](#_Toc412474477)

List of Tables

[Table 1. Key Symbols and Elements 1](#_Toc410051092)

[Table 2. Average Bandwidth Used by Secure Browser for Testing 4](#_Toc410051093)

[Table 3. Ports for Test Delivery System 6](#_Toc410051094)

[Table 4. Wireless Access Points 8](#_Toc410051095)

[Table 5. Flash Requirements 12](#_Toc410051096)

[Table 6. Packages that Include Supported Voice Packs on Linux Distributions 37](#_Toc410051097)

[Table 7. Voice Packs Recognized by Secure Browsers—Windows 38](#_Toc410051098)

[Table 8. Voice Packs Recognized by Secure Browsers—Mac OS X 39](#_Toc410051099)

[Table 9. Voice Packs Recognized by Secure Browsers—Linux 40](#_Toc410051100)

Introduction to the Technical Specifications Manual

This manual provides information about supported operating systems and related requirements, network and Internet requirements, general hardware and software requirements, and text-to-speech information.

## Manual Content

Below is a brief description of each section in this manual, as well as common symbols and elements used throughout the document.

* Section I, Network and Internet Requirements, provides information about bandwidth, networking, and available diagnostic tools.
* Section II, General Software Requirements, outlines required configurations for desktop operating systems (Windows, Mac, and Linux).
* Section III, Text-to-Speech Requirements, contains information for ensuring text-to-speech settings are enabled on desktop operating systems. Information about voice packs for Windows is also included.
* The [appendices](#_Appendix_A._Systems) contain URLs for systems provided by the American Institutes for Research and a checklist for system administrators and technology coordinators.

Table 1. Key Symbols and Elements

| Element | Description |
| --- | --- |
|  | **Warning:** This symbol accompanies important information regarding actions that may cause fatal errors. |
|  | **Alert:** This symbol accompanies important information regarding a task that may cause minor errors. |
|  | **Note:** This symbol accompanies additional information that may be of interest. |
| **text** | Bold text indicates a link or button that is clickable. |
|  | **Tip:** This symbol accompanies suggestions that may be useful. |

## Other Resources

* For information about installing secure browsers, refer to the Secure Browser Installation Manual.
* For information about operating system and general hardware requirements, refer to the Online System Requirements for Ohio Science and Social Studies Tests.

The above resources as well as test administration manuals and user guides for other systems are available on the OCBA (Ohio Computer Based Assessments) portal (http://oh.portal.airast.org/ocba/).

# Network and Internet Requirements

The information in this section provides an overview of network and Internet configuration requirements and available diagnostic tools.

## General Requirements

A stable, high-speed (wired or wireless) Internet connection is required for online testing. The response time for each assessment depends on the reliability and speed of your school’s Internet network.

If your Internet connection is not working or stops working, students will need to complete their tests at a later time or on another day. Any answers they have already submitted will be saved, and students will resume their tests where they left off.

For the online testing applications to work properly, you may need to verify your network settings. If you are not sure whether your network is properly configured or you have questions, contact your network administrator or technology specialist to find the right contact person in your area. You may also contact the Ohio Help Desk.

Network configuration settings should include the following:

* Content filters, firewalls, and proxy servers should be configured to allow traffic on the protocols and to the servers listed below.
* Session timeouts on proxy servers and other devices should be set to values greater than the average scheduled testing time. If testing sessions are scheduled for 60 minutes, consider session timeouts of 65–70 minutes. This will help limit network interruptions during testing.
* Data cannot be cached.
* If your client network uses any devices that perform traffic shaping, packet prioritization, or Quality of Service, the URLs for the systems provided by AIR should be given a high priority to guarantee the highest level of performance.

For information about URLs that should be open or whitelisted, refer to Systems and URLs Provided by AIR.

## Common Network Performance Bottlenecks

All network communications are accomplished using the IP protocol suite. The local area network (LAN) must be able to route IP traffic to and from the Internet.

The Test Delivery System is delivered directly through the Internet. Students must access their tests using the appropriate secure browser. For testing to take place, all workstations where tests will be administered must have reliable Internet connectivity.

In general, the performance of the Test Delivery System will depend on a number of factors, including bandwidth, total number of students simultaneously testing, size of test content, secure browser installation, proxy server (if used), and the wireless networking solution (if used).

### Bandwidth

Bandwidth is the measure of the capacity of a network. Utilized bandwidth measures the amount of data traveling across the network at a given point in time. Bandwidth performance can be affected on either the internal network (LAN) traffic or the Internet traffic from the router. Regardless of hardware or network topology, the LAN should be analyzed to determine the potential for traffic bottlenecks.

The following table displays the estimated average bandwidth used by the secure browser for testing. (Note that there is a one-time exception to these averages; during initial secure browser startup, the load can be greater, leading to a longer load time.) All numbers provided are based on rigorous testing using Wireshark.

Table 2. Average Bandwidth Used by Secure Browser for Testing

| Number of Students Testing Concurrently in School/Building | Average Estimated Bandwidth Consumed During Subsequent Startup of Secure Browsera | Average Estimated Bandwidth Consumed During Testingb |
| --- | --- | --- |
| 1 | 8K bits/second | 5–15K bits/second |
| 50 | 400K bits/second | 250–750K bits/second  (0.25–0.75M bits/second) |
| 100 | 800K bits/second | 500–1500K bits/second  (0.5–1.5M bits/second) |
| a Bandwidth consumed when opening the secure browser and accessing an assessment for the first time is significantly higher than when opening the secure browser and accessing an assessment subsequently. The reason for this is that the initial launch of the secure browser downloads non-secure cacheable content (not test content) that can be immediately accessed upon opening the secure browser at a later time.  b Bandwidth will vary during a student’s testing experience, as some pages contain low-bandwidth content, such as multiple-choice items, and other pages contain higher-bandwidth content, such as animations. Consequently, the estimated average values in this column are based on computing averages from multiple assessments and subjects. | | |

#### Determining Bandwidth Requirements

Schools need to factor the bandwidth requirements of each assessment along with all other non-testing-related Internet traffic in order to determine how many concurrent test sessions their Internet connections can support.

* Some assessments include animations and interactive item types. These may increase the bandwidth required, but the bandwidth should not exceed the peak usage experienced when the test initially loads. **We encourage you to run the diagnostics on your network to determine how many students you can reasonably test at one time.** For information about running diagnostics on your network, refer to the Network Diagnostic Tools section.
* For wired networks, internal bandwidth is typically not a problem, because new switches generally operate at speeds of between 100M bits per second and 1000M bits per second. However, LAN performance can be hindered in cases where hubs are used instead of switches. A hub device will allow broadcast signals from various network devices to propagate across the network, potentially saturating the network and causing traffic competition and/or collisions of data.
* For Internet networks, the most common bottleneck is the ISP’s router connection, which typically operates at speeds of between 1.5M bits per second and 100M bits per second. Network administrators should spend time prior to test administration determining whether their Internet infrastructure has the capacity to accommodate current and future growth.

|  |  |
| --- | --- |
|  | **Analyzing Infrastructure**  Determining whether infrastructure is capable of current and future growth involves a number of steps, including but not limited to: (1) the analysis of the current number of users; (2) current day-to-day Internet bandwidth statistics; and (3) the desired response time for applications. |

#### Total Number of Students Simultaneously Testing

As the number of students testing at one time increases, competition for network bandwidth increases. Network bandwidth resembles highway traffic; as the number of cars traveling on a given road increases, the speed of traffic flow decreases.

#### Size of the Test Content

The size of the test is determined by two factors: (1) the number of items on the test and (2) the average size of each item. The more items a test contains and the larger the average size of a test item, the higher the bandwidth requirement for a given test. For example, ELA tests typically deliver all items associated with a passage at one time, and this may slightly impact the bandwidth for these tests.

### Secure Browser Installation

The recommended installation of the secure browser is local installation on each individual testing workstation. It is possible to install the secure browser on a network or shared drive and then have the testing workstations run the secure browser from that drive, but there may be some performance impacts under this configuration. There will be competition for network bandwidth, and the network or shared disk drive will also be subject to some resource competition as there will be multiple clients reading from the network drive, thus slowing the overall processing speed. See the *Secure Browser Installation Manual* for guidance.

## Network Configuration

### Protocols

All communication with the Test Delivery System takes place over the following Internet port/protocol combinations. Please ensure that the following ports are open for these systems.

Table 3. Ports for Test Delivery System

| Port/Protocol | Purpose |
| --- | --- |
| 80/tcp | HTTP (initial connection only) |
| 443/tcp | HTTPS (secure connection) |

### Domain Name Resolution

All system URLs must be resolvable by all client hosts attempting to connect to the Test Delivery System. This means that the client workstations should be able to convert the friendly names (URLs) to their corresponding IP address by requesting the information from the DNS server.

For a list of URLs, refer to Appendix A, Systems and URLs Provided by AIR.

### Content Filter, Firewalls, and Proxy Servers

Content filters, firewalls, and proxy servers should be configured to allow traffic on the protocols listed above to the applications’ servers.

In addition, session timeouts on proxy servers and other devices should be set to values greater than the average duration it takes a student to participate in a test session or complete a given test. For example, if your school determines that students will test in 75-minute sessions, then consider setting the session timeout to 80 or 85 minutes.

System administrators will need to make sure that information is not blocked in their content filters and that data are not cached. The URLs listed in Appendix A should be open for these systems.

### Quality of Service (QoS)/Traffic Shaping

If the client network utilizes any devices that perform traffic shaping, packet prioritization, or Quality of Service, the URLs should be given a high level of priority in order to guarantee the highest level of performance.

### Certificate Revocation List

Schools should open their firewalls to allow the secure browser to check the certificate authenticity at Symantec Certificate Revocation List (CRL) at <http://crl.verisign.com/>.

#### Symantec Recommendations

Note: The following information was provided by [*Symantec*](https://knowledge.verisign.com/support/mpki-for-ssl-support/index?page=content&id=AD660&actp).

It is strongly recommended that any firewall policies and/or access control devices use URLs and not IP addresses. Symantec can change these IP addresses at any time without notification. If possible, white list the following entries on your firewall policies and/or access control devices to ensure seamless access to our Online Certificate Status Protocol (OCSP) services:

* \*.thawte.com
* \*.geotrust.com
* \*.ws.symantec.com

Note: If white listing wildcard entries is not permitted, you can white list the following specific fully qualified domain names (FQDNs):

* oscp.ws.symantec.com
* oscp.geotrust.com
* oscp.thawte.com

If your firewall is configured to allow only a certain set of IP addresses to be accessed from your network, you will need to take the following actions:

* [Get the full list of IP addresses for the new sites](https://forms.ws.symantec.com/cgi-bin/go.cgi?a=G6EC3-2177-01-26). Complete a short form and then you will gain access to the site list.
* Install or add the IP addresses to your existing list. Do not replace the old IP addresses and do not delete your existing rules for Symantec OCSP IP addresses.

## Wireless Networking

Over the past several years, there have been several revisions to wireless networking technology.

* 802.11n is the fastest and most recent IEEE wireless standard, with a throughput of up to 300M bits per second.
* 802.11g has a theoretical throughput of up to 54M bits per second.
* 802.11b has a theoretical throughput of 11M bits per second.

|  |  |
| --- | --- |
|  | Wireless Security  Due to the sensitivity of test-related data, it is highly recommended that wireless traffic use WPA2/AES data encryption. Because encryption/decryption is part of the data exchange process, there may be a slight decrease in the overall speed of the network. A properly configured wireless network should provide adequate bandwidth for the testing applications. |

### Wireless Access Points

AIR recommends that schools maintain a ratio of wireless systems to wireless access points (WAPs) of no more than 20 to 1. Typically, the test performance begins to deteriorate after that threshold has been reached. In some instances, older WAPs may also see performance degradation when more than 15 devices are concurrently connected.

Recommendations on the optimal number of student workstations per wireless connection

The optimal (or maximum) number of student workstations (computers and tablets) supported by a single wireless connection will depend on the type of networking standard being used for the connection. The two most common networking standards are 802.11g (54Mbps) and the newer and faster standard, 802.11n (300Mbps). Both the access point, which emits the wireless signal, and the computer’s wireless card, which receives the signal, will use one of these two standards. The recommendations in Table 4 are based on the standard in use.

Table 4. Wireless Access Points

|  | 802.11g Access Point | 802.11n Access Point |
| --- | --- | --- |
| 802.11g Wireless Cards | 20 workstations or devices | 40 workstations or devices |
| 802.11n Wireless Cards | 20 workstations or devices | 40 workstations or devices |
| Mix of 802.11g and 802.11n Wireless Cards | 20 workstations or devices | 40–50 workstations or devices (depending on the ratio of wireless cards used) |

|  |  |
| --- | --- |
|  | **Note:** Refer to your WAP documentation for specific recommendations and guidelines. Networks using wireless standards other than 802.11g and 802.11n may also work, but early testing using the practice tests is recommended. |

## Network Diagnostic Tools

A performance analysis of the LAN/Internet infrastructure is recommended in order to identify any bottlenecks that may impact test performance. Identifying the diagnostic tool most appropriate for a network depends on the testing operating system, the network administrator’s knowledge base and the desired level of network analysis. A number of network diagnostic tools are available. These include the following:

### AIR’s Network/Bandwidth Diagnostic Tool

AIR provides a diagnostic tool that can be directly accessed from the student practice test login page.

1. On the practice test login page, click the **Run Diagnostics** link. The Diagnostic Screen page will display.
2. In the Network Diagnostics section, select a test.
3. Select the approximate number of students who may take that test at one time.
4. Click the **Run Network Diagnostics Tests** button.

The results will display your current upload and download speed as well as a general idea of whether you can reliably test the given number of students (the number entered in step 3). You may want to run this test several times throughout the day to verify that your upload and download speeds remain relatively consistent.

### Microsoft Windows Specific Tools

PRTG Traffic Grapher

PRTG ([www.paessler.com/prtg](http://www.paessler.com/prtg)) monitors bandwidth usage and other network parameters via Simple Network Management Protocol (SNMP). It also contains a built‐in packet sniffer. A freeware version is available.

NTttcp

NTttcp ([www.microsoft.com/whdc/device/network/TCP\_tool.mspx](http://www.microsoft.com/whdc/device/network/TCP_tool.mspx)) is a multithreaded, asynchronous application that sends and receives data between two or more endpoints and reports the network performance for the duration of the transfer.

Pathping

Pathping is a network utility included in the Windows operating system. It combines the functionality of Ping with that of Traceroute (Windows filename: tracert) by providing details of the path between two hosts and Ping‐like statistics for each node in the path based on samples taken over a time period.

### Mac OS X Specific Tools

Network Utility.app

This tool is built into Mac OS X software.

### Multi‐Platform Tools

Wireshark

Wireshark ([www.wireshark.org](http://www.wireshark.org)) is a network protocol analyzer. It has a large feature set and runs on most computing platforms including Windows, OS X, Linux, and UNIX.

TCPDump

TCPdump (<http://sourceforge.net/projects/tcpdump>) is a common packet sniffer that runs under the command line and is compatible with most major operating systems (UNIX, Linux, Mac OS X). It allows the user to intercept and display data packets being transmitted or received over a network.

A Windows port WinDump is also available ([www.winpcap.org/windump/](http://www.winpcap.org/windump/)).

Ping, NSLookup, Netstat, Traceroute

This is a set of standard UNIX network utilities. Versions of these utilities are included in all major operating systems (UNIX, Linux, Windows, and Mac OS X).

Iperf

Iperf (<http://sourceforge.net/projects/iperf/>) measures maximum TCP bandwidth, allowing the tuning of various parameters and User Datagram Protocol (UDP) characteristics. Iperf reports bandwidth, delay jitter, and datagram loss.

# General Software Requirements

In addition to installing the secure browser, you may need to adjust operating system settings or install additional software on students’ machines that are used for testing.

## Requirements for All Systems

### Enabling Pop-Up Windows

All systems provided by AIR except for the secure browser require pop-up windows to be enabled. These systems use pop-up windows to provide warning or error messages to users.

Navigate to the appropriate menu option to globally disable pop-up blockers.

To globally enable pop-up windows:

* **Firefox:** Tools > Options > Content > clear **Block pop-up windows**.
* **Google Chrome:** Menu > Settings > Show advanced settings (at the bottom of the screen) > Privacy > Content Settings > Pop-ups > mark **Allow all sites to show pop-ups**.
* **Chrome browser on Android tablets:** Menu > Settings > Advanced > Content Settings > Block pop-ups > clear checkbox.
* **Internet Explorer:** Tools > Pop-up Blocker > Turn Off Pop-up Blocker.
* **Safari:** Application Menu (Safari) > clear **Block Pop-Up Windows**.
* **iOS Safari:** Settings > Safari > Block Pop-ups (toggle to off mode)

If you want only allow certain sites to have pop-up windows, you can add exceptions and whitelist AIR’s systems. For URLs and information about whitelisting, refer to Appendix A, Systems and URLs Provided by AIR.

To add exceptions to the pop-up blocker:

* **Firefox:** Tools > Options > Content > click **Exceptions**. Enter the URL or whitelist protocol for each system.
* **Google Chrome:** Menu > Settings > Show advanced settings (at the bottom of the screen) > Privacy > Content Settings > Pop-ups > click **Manage Exceptions**. Enter the URL or whitelist protocol for each system and select **Allow**. This option is not available for the Chrome browser on Android tablets.
* **Internet Explorer:** Tools > Pop-up Blocker > Pop-up Blocker Settings. Enter the URL or whitelist protocol for each system and click **Add**. Configure other settings as desired.
* Safari and iOS Safari: N/A

### Flash Information

Some test items include animations. Animations can be rendered in Flash or HTML5. Table 5 lists the requirements for installing Flash on the testing computers.

Table 5. Flash Requirements

| Browser | Flash Requirement |
| --- | --- |
| Secure browser 7.0 and later | Renders using HTML5, no need for additional installation. |
| Secure browser 6.5 | Flash bundled in the secure browser installation pack. |
| Secure TestApp | Renders using HTML5, no need for additional installation. |
| Commercial browser\* with HTML5 | Renders using HTML5, no need for additional installation. |
| Commercial browser\* before HTML5 | Install Flash for your operating system, or install the Flash plug-in for the browser. |
| \*Commercial browsers—the versions of Internet Explorer, Firefox, Chrome, Safari, and mobile browsers listed in the Online System Requirements for Ohio Science and Social Studies Tests. | |

## Windows Requirements

This section contains information specific to Windows users.

### Disabling Fast User Switching

Microsoft Windows (XP, Vista, 7, 8.0, and 8.1) allows computers to be configured to allow multiple users to log in to a computer without requiring one user to log out before another logs in. This feature is called “Fast User Switching” and presents a test security risk if it is enabled.

If a student can access multiple user accounts from a single computer, you are required to disable the Fast User Switching function. Instructions for disabling Fast User Switching in Windows XP, 7, and 8 follow.

#### Disabling Fast User Switching in Windows XP

|  |  |
| --- | --- |
| 1. Click Start, click Control Panel, then click User Accounts. 2. Click Change the Way Users Log On or Off.    1. Mark the **Use the Welcome Screen** checkbox.    2. Clear the **Use Fast User Switching** checkbox. 3. Click **Apply Options**.   \*Please note that Fast User Switching is not an option if joined to a domain. |  |

#### Disabling Fast User Switching in Windows 7

The instructions for disabling Fast User Switching in Vista are very similar.

Option A: Access the Group Policy Editor

|  |  |
| --- | --- |
| 1. Click **Start**, type gpedit.msc in the **Start Search** dialog box, and press **Enter**. 2. Navigate to the following location: Local Computer Policy > Computer Configuration > Administrative Templates > System > Logon. 3. Click Hide entry points for Fast User Switching, select Enabled, and click OK. 4. Close the Fast User Switching window. 5. Close the Local Group Policy Editor window.   Note: Because the Group Policy Editor does not exist in certain editions of Windows Vista, you may need to configure these settings via the registry if the above method is unavailable. See below for registry instructions. |  |

Option B: Access the Registry

|  |  |
| --- | --- |
| 1. Click **Start**, type **regedit.exe** in the **Start Search** dialog box, and press **Enter**. 2. Navigate to the following location: HKEY\_LOCAL\_MACHINE > SOFTWARE > Microsoft > Windows > CurrentVersion > Policies > System. 3. Right-click the **System** folder. 4. Click New, DWORD (32-bit) value. 5. Type in HideFastUserSwitching and press Enter. 6. Click the HideFastUserSwitching value. 7. Type **1** into the **Value data** box and click **OK**. 8. Close the Registry Editor window. |  |

#### Disabling Fast User Switching in Windows 8.0 and 8.1

|  |  |
| --- | --- |
| 1. Navigate to the Search option. (From the home screen, mouse to the lower right corner and then click the Search icon.) 2. In the search box, type **gpedit.msc**. Double-click the gpedit icon in the Apps pane. The Local Group Policy Editor window will open. 3. Navigate to the following location: Computer Configuration > Administrative Templates > System > Logon. 4. In the Setting pane, double-click **Hide entry points for Fast User Switching**. | fast-user-switching-in-windows8.jpg |
| 1. Select **Enabled** and then click **OK**. | Hide entry points for Fast User Switching |
| 1. Navigate to the Search option (from the home screen, mouse to the lower right corner and then click the Search icon. 2. In the search box, type **run**. The Run dialogue box will open. 3. Enter the command **gpupdate /force** into the text box and then click **OK**. (Note the space before the backslash.) | Run |
| 1. The Windows system command box will open. When you see the message Computer Policy update has completed successfully, then Fast User Switching has been successfully disabled. | command-prompt-in-windows8.jpg |

### Enabling Web Fonts in Internet Explorer 10 and 11

If students use Internet Explorer 10 or 11 to access the practice tests, web fonts may need to be enabled in order for some item types to display properly.

Enabling Web Fonts in Internet Explorer:

|  |  |
| --- | --- |
| 1. Open the **Tools** menu in Internet Explorer and click **Internet Options**. The Internet Options window will open. 2. Click the **Security** tab. 3. Click the **Custom Level** button. The Security Settings window will open. |  |
| 1. Scroll to **Font Download** in the Settings list and click the **Enable** radio button. 2. Click **OK**. The Security Settings Window will close. 3. Click **OK**. The Internet Options window will close. |  |

### Installing Windows Media Pack for Windows 8.1 N and KN

Some versions of Windows 8.1 are not shipped with media software installed. As a result, you may need to install software in order for students to listen to audio.

Microsoft provides additional information as well as a download package for computers with the following Windows 8.1 versions:

* Windows 8.1 N
* Windows 8.1 N/K with Bing
* Windows 8.1 Enterprise N
* Windows 8.1 Pro N
* Windows 8.1 Pro N/K for EDU

AIR encourages downloading this software and ensuring it works with sample websites and video and audio files prior to installing the Windows secure browser. Installation instructions are provided on Microsoft’s download page.

Microsoft Resources:

* [About the Media Feature Pack for Windows 8.1 N and Windows 8.1 KN Editions: April 2014](http://support.microsoft.com/kb/2929699/en-us) (http://support.microsoft.com/kb/2929699/en-us)
* [Download Media Feature Pack for N and KN Versions of Windows 8.1](http://www.microsoft.com/en-us/download/details.aspx?id=42503) (http://www.microsoft.com/en-us/download/details.aspx?id=42503)

## Mac OS X Requirements

This section contains information specific to Mac OS X users. These settings can be configured before or after installing the secure browser.

### Disabling Spaces

Mac OS X 10.7 through 10.10 includes a Spaces feature that allows running more than one desktop session. This is a security risk because students can potentially start a new desktop session during the test, and use that session to search the Internet for answers. The following procedure explains how to disable Spaces on those versions of OS X. (You can disable Spaces quickly from the command line; see Disabling Spaces and Application Launches from the Command Line for details.)

To disable Spaces in Mission Control:

|  |  |
| --- | --- |
| 1. Navigate to Apple 🡪 System Preferences. | Step1.png |
| 1. In System Preferences, click **Keyboard**. The Keyboard window will be displayed. | Step2-2.png |
| 1. Click the **Keyboard Shortcuts** or **Shortcuts** tab. The Keyboard Shortcuts options will be displayed. | Step3.png |
| 1. In the left panel, click **Mission Control**. The right panel will show all Mission Control options. 2. In the right panel, clear the following checkboxes:    * Move left a space    * Move right a space    * Switch to Desktop 1 (this may already be unchecked) | Step5.png |
| 1. To re-enable Spaces, follow steps 1–5 again, and mark the checkboxes for spaces. |  |

### Function Keys and Application Launches

When students use the secure browser for testing, the Test Delivery System conducts regular checks to ensure that other applications are not open. These checks help maintain the integrity of the secure test environment.

Some Mac computers are configured to launch iTunes and other applications by pressing the function keys (e.g., F8) on the keyboard. This section contains information on how to prevent the function keys from directly launching applications, including iTunes. This action will help prevent students from accidentally pressing a function key instead of a key in the number row.

These instructions are based on Mac 10.9 and should be similar for other supported Macs.

To modify the function keys:

|  |  |
| --- | --- |
| 1. Open **System Preferences**. 2. In the Hardware row, click **Keyboard**. The Keyboard window opens. |  |
| 1. In the Keyboard window, mark the **Use all F1, F2, etc. keys as standard function keys**.   You should no longer be able to launch applications with just the function keys.  If you need to launch iTunes or another application, press the Fn key and then press the desired function key. This combination will launch the application.  Important: If a student is testing with the secure browser and presses the Fn key and a function key, this action will open the linked application and result in the test being paused. |  |

Source: <http://support.apple.com/kb/ht3399>

### Disabling Spaces and Application Launches from the Command Line

The sections Disabling Spaces and Function Keys and Application Launches describe how to configure OS X through the desktop. This section describes how to perform those configurations from the command line, which can be faster than working through the desktop. To perform this task, you need to be familiar with logging in to OS X machines through Terminal or other terminal emulator.

To disable spaces and application launches from the command line:

1. Log in to the machine (remote or local) as the user that runs the secure browser.
2. Enter the following commands:

defaults write com.apple.symbolichotkeys AppleSymbolicHotKeys -dict-add 79 "{enabled = 0; value = {parameters = (65535,123, 262144); type = standard; }; }"

defaults write com.apple.symbolichotkeys AppleSymbolicHotKeys -dict-add 80 "{enabled = 0; value = { parameters = (65535, 123, 393216); type = 'standard'; }; }"

defaults write com.apple.symbolichotkeys AppleSymbolicHotKeys -dict-add 81 "{enabled = 0; value = { parameters = (65535, 124, 262144); type = 'standard'; }; }"

defaults write com.apple.symbolichotkeys AppleSymbolicHotKeys -dict-add 82 "{enabled = 0; value = { parameters = (65535, 124, 393216); type = 'standard'; }; }"

|  |  |
| --- | --- |
|  | **TIP** You can paste these lines into a text file, and run the file from the command line. |

These commands modify the file ~/Library/‌Preferences/‌com.apple.symbolichotkeys.plist.

1. If you logged in to a computer running OS X 10.8.5 or log out of OS X desktop and then log back in.

If you need to restore Spaces and the default application launchers, repeat steps 4–6. In step 5, change enabled = 0 to enabled = 1.

### Disabling Spaces and Application Launches on Remote Machines

The sections Disabling Spaces, Disabling Spaces and Application Launches from the Command Line, and Disabling Spaces and Application Launches from the Command Line describe procedures for configuring a secure test environment in OS X. This configuration is stored in the file ~/Library/‌Preferences/‌com.apple.symbolichotkeys.plist. If you have many OS X testing machines, it may be easier to push this file to those machines instead of configuring each one individually.

You can push the configuration file to remote machines using a variety of tools, such as the following:

* File Distributor
* Apple’s Active Directory Client and Directory Utility
* Apple’s Open Directory and Profile Manager
* Centrify & PowerBrokers Identity Enterprise
* Apple Remote Desktop

## Linux Requirements

This section contains information specific to Linux users.

### Installing Festival and Sound eXchange (SoX) Software

The following two software programs must be installed on Linux machines: Festival and Sound eXchange (SoX). If this software is not installed, students will not be able to hear the audio in the online assessments even when text-to-speech is enabled.

* To download Festival, click here: <http://www.cstr.ed.ac.uk/projects/festival/>.
* To download SoX, click here: <http://sox.sourceforge.net>.

For more information on enabling text-to-speech settings on Linux machines, refer to Section V, Text-to-Speech Requirements, Linux.

## Mobile Requirements

This section provides a brief overview of the requirements for student testing on tablets and Chromebooks. Complete instructions are provided in the Secure Browser Installation Manual.

The AIRSecureTest mobile secure browsers for iOS and Android tablets and Chromebooks are designed to support a secure testing environment. In addition to installing the secure browser, some device settings may need to be adjusted.

### iOS Requirements

#### Guided Access

Guided Access restricts the iOS to a single application and prevents taking screenshots. This ensures a secure test environment. (You may want to use Single App mode, which is easier to enable and activate than Guided Access; for more details about this configuration, see Configuring Using Autonomous Single App Mode.)

The procedure in this section only enables Guided Access; to activate Guided Access before a test, see the Test Administrator User Guide.

#### Enabling Guided Access

|  |  |
| --- | --- |
| 1. Tap the **Settings** icon to open the Settings application. | http://www.coretechniques.com.au/wp-content/uploads/2012/03/portfolio_ipad_settings_icon.jpg |
| 1. Navigate to General > Accessibility > Learning and tap **Guided Access**. |  |
| 1. Tap **Off**; it will change to **On** (enabled). 2. Set the passcode for Guided Access. This passcode is required to deactivate Guided Access after students are finished testing. (If you do not set the passcode now, you will be prompted to set it later.) To set the passcode:    1. Tap **Set Passcode**.    2. Enter a passcode.    3. Confirm the passcode. (You may want to write down or save this number in a safe place. There is no ability to “retrieve” a forgotten passcode.) |  |

### Configuring Using Autonomous Single App Mode

If you have iOS tablets running version 7.1 or higher, and if you have a Mac running version 10.10 or higher, then you can use Autonomous Single App Mode (ASAM) to quickly create a secure testing environment on all iPads used for testing. (Tablets running a version earlier than 7.1 require Guided Access; for details about this configuration, see Enabling Guided Access.) Compared to Guided Access, ASAM requires less time to prepare for test sessions; there is no need to activate Guided Access on each iPad before each test session.

#### Overview of Autonomous Single App Mode and the Secure Testing Environment

To manage multiple iPads using ASAM, you need the do the following:

Step 1: Creating a Mobile Device Management Profile

Step 1a (Optional): Restricting Features in iOS 8.1.3

Step 2: Creating a Supervisory Profile

Step 3: Placing iPads in Autonomous Single App Mode

After completing these three steps, each time a student starts a test, the iPad enters ASAM and the test environment is secure.

#### Step 1: Creating a Mobile Device Management Profile

The first step in provisioning iPads with ASAM is to create an MDM profile. All default profile settings are compatible. However, you may wish to restrict certain features in iOS 8.1.3 devices (see Step 1a (Optional): Restricting Features in iOS 8.1.3). Deploy the profile to a host that the iPads can access.

Creating an MDM profile is beyond the scope of this specification manual. The following references provide introductory information:

* IT in the Classroom, available at <https://www.apple.com/education/it/mdm/>.
* Apple Configurator Help, available at [https://help.apple.com/configurator/mac/1.0/#](https://help.apple.com/configurator/mac/1.0/).
* Pro tip: Use OS X Server Profile Manager for MDM, available at <http://www.techrepublic.com/article/pro-tip-use-os-x-server-profile-manager-for-mdm/>.

#### Step 1a (Optional): Restricting Features in iOS 8.1.3

You can restrict features in supervised iOS 8.1.3 devices that may give students an unfair testing advantage, including the dictionary, predictive keyboard, spell check, and auto-correction. If you wish to restrict any of these features, you may do so when creating the MDM profile for these devices.

|  |  |
| --- | --- |
|  | **Note:** The current version of Apple Configurator does not allow you to restrict these features. If you wish to restrict these features when configuring the MDM profile, you must use a third-party MDM solution. |

To restrict features in iOS 8.1.3 devices:

* In the Custom Settings section of the MDM solution, insert the profile key for each feature you wish to restrict. Table 7 provides a list of the relevant profile keys.

Table . Profile Keys for iOS 8.1.3 Features

|  |  |  |
| --- | --- | --- |
| Feature | Profile Key | Recommended Value |
| Dictionary | <key>allowDefinitionLookup</key> | False |
| Predictive Keyboard | <key>allowPredictiveKeyboard</key> | False |
| Spell Check | <key>allowSpellCheck</key> | False |
| Auto-Correction | <key>allowAutoCorrection</key> | False |

The following snippet turns off the iPad’s auto-correction feature. The snippets for dictionary, predictive keyboard, and spell check are similar.

<dict>

<key>allowAutoCorrection</key>

<false />

<key>PayloadDisplayName</key>

<string>Restrictions</string>

<key>PayloadDescription</key>

<string>RestrictionSettings</string>

<key>PayloadIdentifier</key>

<string>31eb53ac-3a08-46f7-8a0a-82e872382e15.Restrictions</string>

<key>PayloadOrganization</key>

<string></string>

<key>PayloadType</key>

<string>com.apple.applicationaccess</string>

<key>PayloadUUID</key>

<string>56199b2c-374d-4152-bc50-166d21fa9152</string>

<key>PayloadVersion</key>

<integer>1</integer>

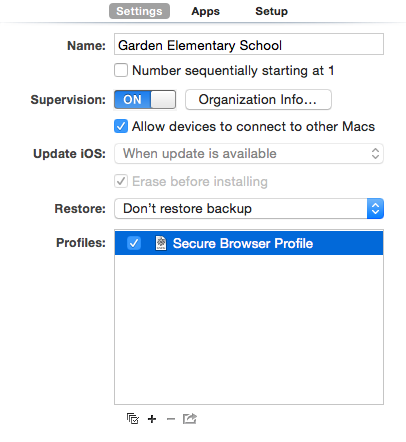
</dict>

#### Step 2: Creating a Supervisory Profile

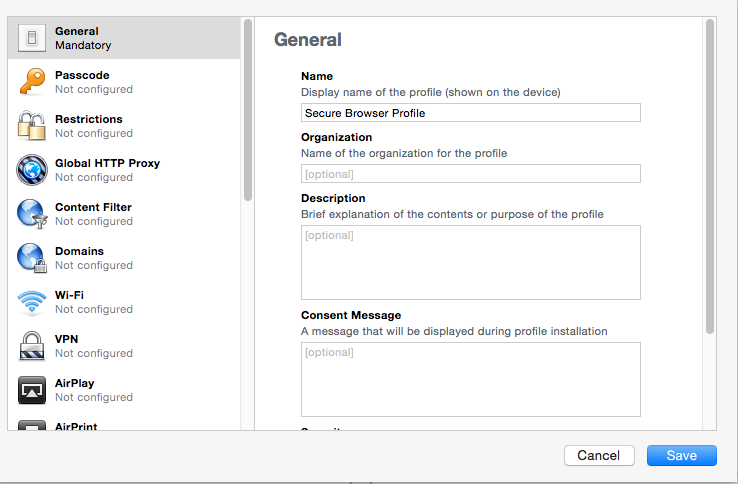
To create a supervisory profile:

1. On a Mac 10.10, download and install Apple Configurator from the Mac App Store. When the installation completes, open Apple Configurator.
2. Click **Prepare**, then **Settings**. The Settings window appears.

Figure 1. Settings Window in Apple Configurator



1. Click **+** below the Profiles list and select **Create New Profile…**. A configuration window appears.



1. In the **General** section, in the Name field, enter a name for the profile.
2. In the **Restrictions** section, click **Configure**. A list of restrictions appears.
3. Make any required changes to the restrictions, or retain the defaults settings.
4. Click **Save**. You return to the Settings tab, and the profile appears in the Profiles list.
5. Click  to export the profile to the Mac.

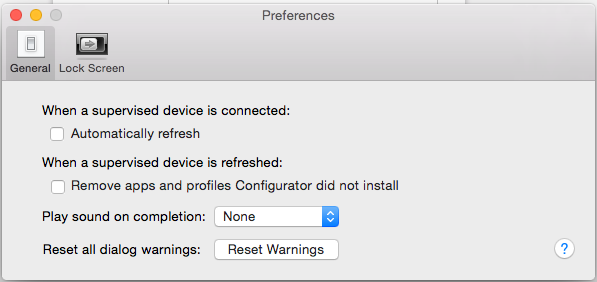
Creation of the supervisory profile is complete.

#### Step 3: Placing iPads in Autonomous Single App Mode

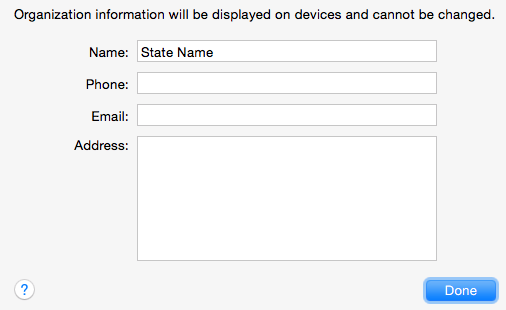
|  |  |
| --- | --- |
|  | **TIP: Installing on multiple iPads at once** Before starting this procedure, connect the iPads to the Mac through a USB hub. That way you can perform the installation on many of them at one time. |

To install the MDM profile, supervisory profile, and secure browser:

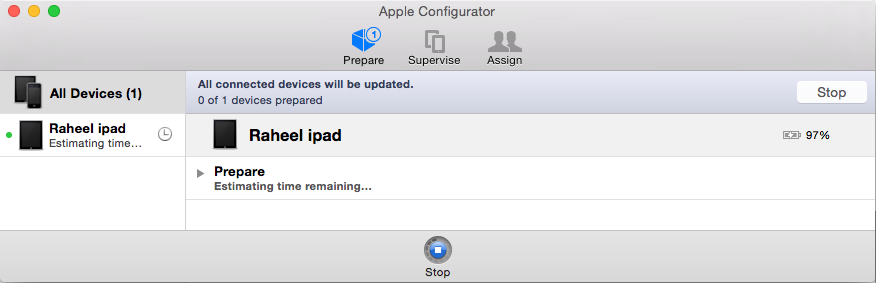
1. On the Mac where you performed Step 2: Creating a Supervisory Profile, open the Apple Configurator.
2. From the **Apple Configurator** menu, select **Preferences**. The Preferences window opens.



1. Under **General**, clear the **Automatically refresh** and **Remove apps and profiles Configurator did not install** checkboxes.
2. Close the Preferences window.
3. Back in Apple Configurator, click **Prepare**, then **Settings**. The Settings window appears (see Figure 1).
4. In the Name field, enter a name to apply to the iPads.
5. Optional: Mark the **Number sequentially starting at 1** checkbox. This adds a number to each iPad’s name. For example, if the Name field is Garden Elementary School, and if three iPads are connected, each device receives the name Garden Elementary School 1, Garden Elementary School 2, and Garden Elementary School 3.
6. Set Supervision to **On**.
7. Click **Organization Info…** The Organization Info window appears.



1. In the Organization field, enter Ohio Online and then click **Done**. The Organization Info window closes.
2. If the profile you created in Step 2: Creating a Supervisory Profile does not appear in the Profiles list, import it by doing the following:
   1. Click **+** below the Profiles list and select **Import Profile…**.
   2. Navigate to the profile you saved in step 8 on page 25, and then click **Open**.
3. Mark the checkbox for the profile you want to prepare onto the iPads (see Figure 1).
4. Connect each iPad to the Mac via a USB cable or USB hub.
5. On each connected iPad, uninstall any existing versions of the secure browser.
6. In the Apple Configurator, under the Prepare tab, click **Prepare** at the bottom of the window. A confirmation message appears.
7. Click **Apply** in the confirmation message. Preparation starts and may take several minutes, after which the iPad restarts. The Apple Configurator displays progress messages during the prepare.



|  |  |
| --- | --- |
|  | **Note: iOS Upgrade** Apple Configurator may force the iPads to upgrade to the latest version of iOS. |

1. After the iPad restarts, follow the prompts on the iPad to configure it until the home screen appears.
2. Optional: Confirm the supervisory profile is installed on the iPad. Go to **Settings > General > Profiles**. The profile name you used in step 4 on page 25 appears under Configuration Profiles.
3. On the iPad, download and install the MDM profile you created in Step 1: Creating a Mobile Device Management Profile.
4. After the MDM profile installation completes, install the secure browser onto the iPad. You can take a copy of the secure browser for iOS from http://oh.portal.airast.org/ocba/. (Detailed instructions for installing the secure browser are in the section “Installing the Secure Browser on iOS” of the Secure Browser Installation Manual.)
5. Optional: After installation completes, test it by doing the following:
   1. Open the Secure Browser.
   2. Log into a test site.
   3. Select a test, have the TA approve the test.
   4. Start the test. The iPad enters ASAM.
6. Repeat steps 13–21 to prepare additional iPads.
7. In the Apple Configurator, click **Stop** and close the Apple Configurator.

Setting the iPad into ASAM is complete. When a student starts a test, the iPad enters ASAM mode.

### Android Requirements

The mobile secure browser for Android tablets requires the secure browser keyboard to be selected before students can access the login page. The reason for this is that the default Android keyboard allows predictive text, which would unduly aid students when entering written responses to test items. The secure browser keyboard is a basic keyboard, with no row for predictive text functionality.

The first time you open the Mobile Secure Browser on an Android tablet, you will be prompted to select the secure browser keyboard.

Instructions for enabling the secure browser keyboard follow.

|  |  |
| --- | --- |
|  | **About the Secure Browser Keyboard and General Settings**  Once the secure browser keyboard is set, it becomes the default keyboard for all Android tablet applications, not just the secure browser. If you want to return to the default Android keyboard after using the secure browser, you will need to navigate to Settings > Language & Input and uncheck the secure browser keyboard.  If you change back to the default Android keyboard, you will be prompted to select the secure browser keyboard the next time you open the secure browser. The secure browser will not allow you to access the student login page until the secure browser keyboard has been selected. |

#### Enabling the Secure Browser Keyboard

Note: All screenshots in this section were taken with a Samsung Galaxy Tab 2.

|  |  |
| --- | --- |
| 1. Select the secure browser icon on the home screen. |  |
| 1. You will be prompted to change the keyboard. Select **Close**. |  |
| 1. Select **Set up input methods**. The Language and Input settings screen will automatically open. |  |
| 1. Select the checkbox next to **AIRSecureTest** so that a checkmark appears. 2. You will be prompted to acknowledge that this selection is okay. Select **OK** to continue. Note: This action allows the mobile secure browser to use the secure browser keyboard. |  |
| 1. Navigate to the secure browser to open it. (You can use the application switcher or go back to “Home” and select the secure browser icon.) 2. You will be prompted to change the keyboard. Select **Close**. |  |
| 1. The Android tablet’s default keyboard will still be selected. 2. Select the checkmark or circle for the **AIRSecureTest** keyboard. |  |
| 1. Select **Continue**. You will be prompted to complete the application launch using the preferred method. |  |
| 1. Select AIRSecureTest (ensure it is shaded and highlighted blue) and then select **Always**. 2. You will need to acknowledge that the secure browser’s default settings have changed. (This is a result of selecting the secure browser keyboard.) |  |
| 1. Select **OK**. |  |

### Chrome OS Requirements

The American Institutes for Research has worked with Google to develop a secure browser kiosk application that can be downloaded onto Chromebooks from the Chrome Web Store. Using the AIRSecureTest kiosk application requires Chromebooks to run in kiosk mode.

|  |  |
| --- | --- |
|  | About the AIRSecureTest Kiosk App  The AIRSecureTest browser is not a hosted app. In order to support all test features, AIR developed a packaged kiosk application. As a result, this app must be deployed onto managed Chromebooks via the Chrome Management Console as a kiosk application rather than via a public session. (You may still use public sessions for other applications.) |

Instructions for installing the kiosk application are in the Secure Browser Installation Manual.

#### Google Documentation

The following references are for users who need to ensure that managed Chromebooks are configured correctly prior to installing the AIRSecureTest kiosk app.

##### Managed Chromebooks

* [Using Chromebooks for Student Assessments](https://support.google.com/chrome/a/answer/3273084) (https://support.google.com/chrome/a/answer/3273084)
  + Refer to “Scenario 1: School sets up Chromebook to run as a Single App Kiosk running the exam app.”
  + Do NOT follow the instructions for Scenarios 2 and 3.
* [Managing Device Settings](https://support.google.com/chrome/a/answer/1375678) (https://support.google.com/chrome/a/answer/1375678)

##### Non-Managed Chromebooks

Non-managed Chromebooks must not already be configured with user accounts before you enable kiosk mode. If you have already added user accounts to Chromebooks, you will need to wipe the devices.

Google has provided instructions for wiping Chromebooks: <https://support.google.com/chrome/a/answer/1360642?hl=en>.

After you wipe the Chromebooks, follow the instructions in the Secure Browser Installation Manual to enable kiosk mode and install the AIRSecureTest app.

# Text-to-Speech Requirements

This section contains information about text-to-speech requirements.

## Overview of Text-to-Speech

Using text-to-speech requires at least one voice pack to be pre-installed on computers that will be used for testing. For Windows, Mac, Android, and Chrome operating systems, default voice packs are typically pre-installed. For computers running a Linux distribution, voice packs may need to be downloaded and installed.

A number of voice packs are available for desktop computers, and AIR researches and tests voice packs for compatibility with the secure browsers. Additionally, not all voice packs that come pre-installed with operating systems are approved for use with online testing. The voice packs listed at the end of this section have been tested and are whitelisted by the secure browser.

### Using Text-to-Speech

Students using text-to-speech for the practice tests must log in using a supported secure browser. Students can also verify that text-to-speech works on their computers by logging in to a practice test session and selecting text-to-speech on the Choose Settings screen.

|  |  |
| --- | --- |
|  | **Note:** We strongly encourage schools to test the text-to-speech settings before students take operational tests. You can check these settings by taking a practice test using the secure browser or app, and selecting the Text To Speech option on the Choose Settings page while signing in. |

### How the Secure Browsers Work With Voice Packs

#### Desktop Secure Browsers

The secure browsers are configured to recognize several known voice packs to provide the text-to-speech accommodation. The secure browsers detect pre-installed voice packs on the students’ machines. When a student who is using text-to-speech logs in to a test session and has been approved for testing, the secure browser will look for voice packs on the student’s machine. When it recognizes an approved voice pack, the one with the highest priority rating will be used.

If any of the approved voice packs has also been set as the default voice on the computer, then that voice pack will always get the highest priority.

#### Mobile Secure Browsers

The mobile secure browser uses either the device’s native voice pack or a voice pack embedded in the secure browser. If additional voice packs are downloaded to a tablet or Chromebook, they will not be recognized by the mobile secure browser.

##### iOS

Mobile Secure Browser version 2.2

* iOS 6.0–6.1: The embedded NeoSpeech voice pack will be used.
* iOS 7.0–8.1: The native iOS voice pack will be used.

##### Android

The AIRSecureTest app for Android uses the native voice pack available on the supported Android tablet being used.

##### Chrome OS

The AIRSecureTest kiosk app for Chromebooks uses the native voice pack available on the Chromebook device being used.

### About NeoSpeech™ Voice Packs for Windows

Pursuant to an agreement between NeoSpeech™ and the American Institutes for Research (AIR), authorized users may download and install specific licensed NeoSpeech™ voice packs for use on supported Windows computers (Windows XP Service Pack 3, Vista, 7, 8.0, and 8.1).

These voice packs can be used instead of the default Windows voice packs for English and the commercial Spanish voice packs from Cepstral. (The default Windows voice packs as well as the Cepstral voice packs for Windows may still be used for text-to-speech, if desired.)

* The Julie voice pack is for English text-to-speech users.
* The Violeta voice pack is for Spanish text-to-speech users.

The NeoSpeech™ voice pack is to be used only in conjunction with, and not separate from, the online assessments provided by AIR's Test Delivery System.

The NeoSpeech™ voice packs can be downloaded from TIDE. Installation instructions are also available in TIDE.

## Windows Text-to-Speech Settings

This section explains how to configure Windows for using text-to-speech with the secure browser. The text-to-speech feature is available on Windows versions as listed in the Online System Requirements for Ohio Science and Social Studies Tests.

The instructions in this section are for Windows 7. The process is similar for other versions of Windows.

|  |  |
| --- | --- |
| 1. Open the Control Panel window, and select **Speech Recognition**. 2. In the Speech Recognition window, select **Text to Speech**. |  |
| 1. Configure default text-to-speech preferences.    1. Voice selection: If multiple voice packs are available, select the default voice.    2. Select **Preview Voice** to see whether the selected voice requires a rate adjustment.    3. Voice speed: If necessary, adjust the voice speed. Drag the slider to make the voice speak slower or faster. To listen to the rate, select **Audio Output**.    4. When you are done, click **OK** to save your settings and then close the Speech Properties window. |  |

## Mac OS X Text-to-Speech Settings

This section explains how to configure Mac OS X for using text-to-speech with the secure browser. The text-to-speech feature is available on OS X versions as listed in the Online System Requirements for Ohio Science and Social Studies Tests.

The instructions in this section are for OS X 10.9. The process is similar for other versions of OS X.

|  |  |
| --- | --- |
| 1. Open System Preferences, and select **Dictation & Speech**. |  |
| 1. In the Text to Speech section, configure your default text-to-speech preferences.    * System Voice: If multiple voice packs are available, select the default voice.    * Select **Play** to see whether the selected voice requires a rate adjustment.    * Speaking Rate: If necessary, adjust the voice speed. Drag the slider to make the voice speak slower or faster. To listen to the rate, select **Play**.    * When you are done, click the red **X** in the upper left corner to save your settings and close the Speech window. |  |

## Linux Text-to-Speech Settings

This section explains how to install voice packs on the supported Linux distributions.

1. Install Festival for text-to-speech:
   * Ubuntu: sudo apt-get install festival
   * Fedora, RedHat: yum install festival
   * openSUSE: zypper install festival
2. Install SoX for text-to-speech:
   * Ubuntu: sudo apt-get install sox
   * Fedora, RedHat: yum install sox
   * openSUSE: zypper install festival
3. Using Table 6 as a reference, install voice packs from the indicated packages. (These are the supported voice packs.)

Table 6. Packages that Include Supported Voice Packs on Linux Distributions

| Distribution/Voice Pack | Available in Package |
| --- | --- |
| Ubuntu | |
| kal\_diphone (Kevin American English male) | festvox-kallpc16k, festvox-kallpc8k |
| ked\_diphone (Kurt American English male) | festvox-kdlpc16k, festvox-kdlpc8k |
| el\_diphone (Castilian Spanish male) | festvox-ellpc11k |
| openSuse | |
| kal\_diphone (Kevin American English male) | (included in festival) |
| Fedora, RedHat | |
| cmu\_us\_awb\_arctic\_hts (Scottish English male) | festvox-awb-arctic-hts |
| cmu\_us\_bdl\_arctic\_hts (American English male) | festvox-bdl-arctic-hts |
| cmu\_us\_jmk\_arctic\_hts (Canadian English male speaker) | festvox-jmk-arctic-hts |
| kal\_diphone (Kevin American English male) | festvox-kal-diphone |
| ked\_diphone (Kurt American English male) | festvox-ked-diphone |

## Voice Packs Recognized by Desktop Secure Browsers

The tables in this section display the voice packs for each desktop operating system (Windows, Mac, and Linux) that are currently recognized by the secure browser.

Windows and Mac OS X computers typically ship with at least one default voice pack. Many of these default voice packs are recognized by the secure browser.

### Windows

Table 7. Voice Packs Recognized by Secure Browsers—Windows

| Vendor | Voice Pack | Language |
| --- | --- | --- |
| Windows (pre-installed) | Julie | English |
| Windows (pre-installed) | Kate | English |
| Windows (pre-installed) | Michael | English |
| Windows (pre-installed) | Michelle | English |
| Windows (pre-installed) | MSAnna | English |
| Windows (pre-installed) | MS\_EN-GB\_HAZEL | English |
| Windows (pre-installed) | MS\_EN-US\_DAVID | English |
| Windows (pre-installed) | MS\_EN-US\_ZIRA | English |
| Windows (pre-installed) | MSMary | English |
| Windows (pre-installed) | MSMike | English |
| Windows (pre-installed) | MSSam | English |
| Windows (pre-installed) | Paul | English |
| Windows (pre-installed) | Violeta | Spanish |
| Cepstral (commercial) | Cepstral\_David | English |
| Cepstral (commercial) | Cepstral\_Marta | Spanish |
| Cepstral (commercial) | Cepstral\_Miguel | Spanish |
| NeoSpeech (commercial) | VW Julie | English |
| NeoSpeech (commercial) | VW Violeta | Spanish |

### Mac OS X

Table 8. Voice Packs Recognized by Secure Browsers—Mac OS X

| Vendor | Voice Pack | Language |
| --- | --- | --- |
| Mac (pre-installed) | Agnes | English |
| Mac (pre-installed) | Alex | English |
| Mac (pre-installed) | Bruce | English |
| Mac (pre-installed) | Callie | English |
| Mac (pre-installed) | David | English |
| Mac (pre-installed) | Fred | English |
| Mac (pre-installed) | Jill | English |
| Mac (pre-installed) | Junior | English |
| Mac (pre-installed) | Kathy | English |
| Mac (pre-installed) | Princess | English |
| Mac (pre-installed) | Ralph | English |
| Mac (pre-installed) | Samantha | English |
| Mac (pre-installed) | Tom | Spanish |
| Mac (pre-installed) | Vicki | English |
| Mac (pre-installed) | Victoria | English |
| Mac (pre-installed) | Diego | Spanish |
| Mac (pre-installed) | Javier | Spanish |
| Mac (pre-installed) | Marta | Spanish |
| Mac (pre-installed) | Monica | Spanish |
| Mac (pre-installed) | Paulina | Spanish |
| Infovox (commercial) | Heather Infovox iVox HQ | English |
| Infovox (commercial) | Rosa Infovox iVox HQ | Spanish |

### Linux

Table 9. Voice Packs Recognized by Secure Browsers—Linux

| Vendor | Voice Pack | Language |
| --- | --- | --- |
| Festvox (commercial) | cmu\_us\_awb\_arctic\_hts | English |
| Festvox (commercial) | cmu\_us\_bdl\_arctic\_hts | English |
| Festvox (commercial) | cmu\_us\_jmk\_arctic\_hts | English |
| Festvox (commercial) | cmu\_us\_slt\_arctic\_hts | English |
| Festvox (commercial) | kal\_diphone | English |
| Festvox (commercial) | ked\_diphone | English |

1. Systems and URLs Provided by AIR

This appendix provides information about the URLs for each system that AIR provides.

## Non-Testing Sites

| System | URL |
| --- | --- |
| Portal and secure browser installation files | oh.portal.airast.org |
| Single Sign On System | oh.sso.airast.org |
| Test Information Distribution Engine | oh.tide.airast.org |
| Online Reporting System | oh.ors.airast.org |

## Testing Sites

### TA and Student Testing Sites

The Test Administrator and student testing sites use a cloud-based satellite system for optimal load balancing during testing. This includes the operational sites (TA Interface and Student Testing Site) and practice sites (TA Practice Site and Practice Test Site). Testing servers and satellites may be added or modified during the school year to ensure an optimal testing experience. As a result, AIR strongly encourages you to whitelist at the root level. This requires using a wildcard.

| System | URL |
| --- | --- |
| TA and Student Testing Sites | \*.tds.airast.org |

1. Technology Coordinator Checklist

You can use this checklist during review of networks and computers used for testing.

|  | Activity | Target Completion Date | Reference |
| --- | --- | --- | --- |
|  | Verify that all of your school’s computers that will be used for online testing meet the operating system requirements. | 3–4 weeks before testing begins in your school | Online System Requirements for Ohio Science and Social Studies Tests |
|  | Verify that your school’s network and Internet are properly configured for testing, conduct network diagnostics, and resolve any issues. | 3–4 weeks before testing begins in your school | Network and Internet Requirements |
|  | Install the secure browser on all computers that will be used for testing. | 3–4 weeks before testing begins in your school | Secure Browser Installation Manual |
|  | Enable pop-up windows and review software requirements for each operating system. | 1–2 weeks before testing begins in your school | General Software Requirements |
|  | On **Windows** computers, disable Fast User Switching.  If a student can access multiple user accounts on a single computer, you are encouraged to disable the Fast User Switching function. | 1–2 weeks before testing begins in your school | Disabling Fast User Switching |
|  | On **Mac 10.7—10.10** computers, disable Spaces in Mission Control. | 1–2 weeks before testing begins in your school | Disabling Spaces |
|  | Install and verify any required text-to-speech software onto computers that will be used for testing. | 1–2 weeks before testing begins in your school | Text-to-Speech Requirements |
|  | On iPads, Androids and Chromebooks, complete the Launchpad step. | 1–2 weeks before testing begins in your school | Secure Browser Installation Manual |
|  | On **iPads**, ensure that Guided Access or ASAM is enabled and that TAs know how to activate Guided Access. | 1–2 weeks before testing begins in your school | Enabling Guided Access |
|  | On **Android** tablets, ensure that the secure browser keyboard is enabled. | 1–2 weeks before testing begins in your school | Enabling the Secure Browser Keyboard |

1. User Support

If this document does not answer your questions, please contact the Ohio Help Desk.

The Help Desk will be open Monday–Friday from 7:00 a.m. to 5:00 p.m. (except holidays).

|  |
| --- |
| **Ohio Help Desk**  Toll-Free Phone Support: 1-877-231-7809  Email Support: OHHelpDesk@air.org |

If you contact the Help Desk, you will be asked to provide as much detail as possible about the issues you encountered.

Include the following information:

* Test Administrator name and IT/network contact person and contact information
* SSIDs of affected students
* Results ID for the affected student tests
* Operating system and browser version information
* Any error messages and codes that appeared, if applicable
* Information about your network configuration:
  + Secure browser installation (to individual machines or network)
  + Wired or wireless Internet network setup